

**DoD Wireless Push Email System Security Requirements Matrix**  
**Version 2.0**  
**June 1, 2007**

Requirement Number	Requirement	Source of Requirement
	<p>This matrix was developed by the DISA Field Security Operations (FSO) and is an unofficial compilation of DoD security requirements for PDA/smartphone wireless push email systems. The purpose of the matrix is to provide a tool for DISA FSO when evaluating commercial wireless push email systems hosted on PDAs. The requirements listed in this document are subject to change as new security vulnerabilities are identified or DoD commands or agencies provide comments to DISA.</p> <p>This matrix represents security requirements that must be met by technical means. In other words, the PDA/smartphone wireless push email system must include a system capability or feature that meets each security requirement. A deployed DoD PDA/smartphone wireless push email system must also meet additional policy, procedure, and user training requirements, which are not listed in this matrix, but are listed in the appropriate Wireless STIG Checklist.</p> <p>A copy of this matrix will be provided to DoD commands/agencies and vendors upon request (send an email request to <a href="http://fso_spt@disa.mil">http://fso_spt@disa.mil</a>).</p> <p>A wireless email system consists of the following components, some of which may not be included in a wireless email vendor's product.</p> <ul style="list-style-type: none"> <li>– Wireless handheld device (e.g. PDA, Smartphone)</li> <li>– Smart Card Reader and Drivers</li> <li>– Software installed on the handheld device by the device manufacturer or wireless carrier (e.g. operating system, internet browser, productivity applications)</li> <li>– Wireless email product client and server software</li> <li>– Common Access Card (CAC) Middleware</li> <li>– IT Security Policy management server</li> <li>– Gateway server located with the IT policy management server providing connection between the wireless handheld device and corporate network services (optional)</li> </ul> <p>If the wireless email vendor's product does not include all of the features listed in this matrix, additional mobile device IT management, antivirus, and personal firewall software must be used to meet the requirements listed below.</p> <p>Note: Bluetooth Smart Card Reader (SCR) security requirements are listed in a separate document (<b>DoD Bluetooth Smart Card reader Security Requirements Matrix</b>, version 2.0, 1 June 2007).</p> <p><b>Changes from previous version:</b></p> <ul style="list-style-type: none"> <li>-Previous version was 1.3, dated Mar 23, 2007.</li> <li>-Requirement 2.0 (Data Wipe) has been substantially revised and is now called "Data Protection."</li> <li>-Requirement 3.1. Added clarification on required encryption algorithms.</li> <li>-Requirement 6.0. Added clarification information.</li> <li>-Requirement 9.0. Added clarification information.</li> </ul>	

Requirement Number	Requirement	Source of Requirement
<p>-Requirement 10.0. Added clarification concerning certificate based authentication requirement. Previous Requirement 10.1 deleted and previous Requirement 10.2 now is 10.1.</p> <p>-Requirement 21.1.3. Changed "Data Wipe" to "Data Protection."</p> <p>-Requirement 24.0. Changed title from "Content Protection" to "Data-at-Rest Protection."</p> <p>-Requirement 24.2. Added clarification information</p> <p>-Requirement 25.0 (Bluetooth requirements). This section has been substantially revised.</p>		
<b>General Requirements</b>		
1.0	Email redirection from the Exchange Server to the wireless handheld device shall be controlled via centrally managed server. Desktop or Internet controlled email redirection is not authorized.	Wireless STIG, JTF-GNO Technical Bulletins 05-018 and 05-019
2.0	Data Protection  Device data will be protected using the following methods to protect DoD data on the handheld when it is lost or stolen. Either Requirement 2.1 or 2.2 must be implemented. Also, Requirement 2.5 must be implemented.	
2.1	Data Wipe (hard reset) requirements	
2.1.1	The system shall have the capability to perform a "Data Wipe" function whereby all data (operating system, applications, and data) stored in user addressable memory on the handheld device will be erased.	Wireless STIG, JTF-GNO Technical Bulletins 05-018 and 05-019
2.1.2	The system "Data Wipe" function will sanitize all addressable memory locations on the handheld device according to the procedures in the NSA/CSS Policy Manual 9-12 (FOUO).  (Note: This is a highly desired capability, not a requirement. The goal is to sanitize the device after a Classified Message Incident (CMI).)  See Note 1 below	Wireless STIG
2.2	Data Obfuscation	
2.2.1	The system shall encrypt all data (operating system, applications, and data) stored in user addressable memory on the handheld device using a FIPS certified AES-256 encryption algorithm and a FIPS 140-2 certified encryption module.	
2.2.2	When the Data Obfuscation procedure is implemented, the AES encryption key shall be deleted, scrambled, or hidden such that it is no longer available to decrypt the device data.	
2.3	A highly desirable, but not required, feature is the capability to "Data Protect" all removable storage media.	

Requirement Number	Requirement	Source of Requirement
2.4	Remote Data Protection The system shall provide remote data protection capabilities using one or both of the following methods (2.4.1 or 2.4.2):	Wireless STIG, JTF-GNO Technical Bulletins 05-018 and 05-019
2.4.1	The system administrator shall have the capability transmit a remote Data Protection (e.g. "Data Wipe" or "Data Obfuscation") command to the handheld device.	
2.4.2	The system will automatically perform a "Data Protection" procedure ("Data Wipe" or "Data Obfuscation") after a set period of time the device has not contacted the management server.	
2.4.2.1	The required "server no-contact" period shall be configurable from 1 day to 14 days.	
2.5	The system shall enforce user authentication to unlock the device and automatically perform a "Data Protection" procedure after a set number of incorrect authentication attempts occur. See Requirements 21.0 and 30.4 for additional information.	
3.0	Encryption of transmitted data/email	
3.1	All data (including email attachments) sent over the wireless link from the PDA/smartphone to the wireless email server located on the DoD network will be encrypted using FIPS 140-2 validated cryptographic modules. The available encryption algorithms will be restricted to 3DES and/or AES. (Note: Support for AES only may be required by some DoD sites.)	DoDD 8100.2
3.2	All updates / rekeying of the link encryption key used to encrypt email on the wireless link shall be controlled by the wireless email server located on the DoD network	Wireless STIG
3.3	AES shall be available as the master or session key algorithm.	DoDD 8100.2
3.4	The rekey period will be 30 days or less.	Wireless STIG
4.0	S/MIME requirements	
4.1	The system will be capable of providing S/MIME v3 (or later version) encryption of email. FIPS 140-2 validated cryptographic modules will be used by the S/MIME service for data in transit.	DoDD 8500.1, DoDD 8100.2
4.2	S/MIME shall be fully interoperable with DoD PKI and CAC. CAC (hard token) and PKCS#12 (soft token) certificate stores should be supported.	DoDI 8520.2
5.0	If the wireless email system provides text messaging services (e.g. PIN-to-PIN messaging), the service will be S/MIME enabled.	Wireless STIG
5.1	Information sent via available text messaging services should be logged. This is an optional, but recommended capability.	
6.0	If the wireless email service provides wireless activation / provisioning of the handheld device, the following requirements must be met: the system administrator shall have the capability to disable this service. A trusted loading process must be the foundation for device provisioning, whether tethered or over-the-air.	DoD D 8100.2, Wireless STIG

Requirement Number	Requirement	Source of Requirement
6.1	The system administrator shall have the capability to disable OTA provisioning.	
6.2	A trusted loading process must be the foundation for device provisioning (whether tethered or over-the-air).	
6.2.1	The trusted OTA provisioning process must provide mutual authentication between the provisioning server and the provisioned device.	
6.2.2	The trusted OTA provisioning process must provide data integrity and confidentiality of the provisioning data downloaded from the server to the handheld device.	
7.0	Internet connections.	Wireless STIG, JTF-GNO Technical Bulletins 05-018 and 05-019
7.1	The system administrator shall have the capability to remove the wireless carrier's Internet browser icon from the handheld device screen during provisioning of the handheld device or configure the system to satisfy requirement 7.2.	
7.2	The system administrator shall have the capability to configure the browser to connect only to a specific URL (e.g. DoD network VPN gateway, DoD web proxy) during provisioning of the handheld device. The user shall not be able to override this setting.	
7.3	The desire is to require users to browse the Internet through a secure encrypted tunnel (using a FIPS 140-2 validated cryptographic module) to the DoD network Internet gateway.	
8.0	The system shall have the capability to log all security events (e.g. user logon, logoff, system admin configuration changes).	Wireless STIG
8.1	The system shall have the capability to send email alert notifications to the system administrator when specific system log events occur. Optional requirement.	
8.2	The system should have the capability to audit certain Bluetooth-related device-level events that identify changes to security settings, incoming or outgoing connection requests (including Bluetooth device addresses), failed authentication attempts, and other unauthorized activity. This is an optional, but recommended capability.	NSA I332 IA Vulnerability Assessment of RIM Bluetooth SCR.
9.0	A user shall be required to enter user authentication credentials using Smart Card Login (SCL) prior to gaining access to any DoD network services (e.g. internal network web servers) other than push email. (Note: This authentication is separate from user authentication for unlocking the handheld device.)	DoDD 8500.1
9.1	User SCL authentication support for access to network and web services shall be fully interoperable with DoD PKI and CAC.	DoDI 8520.2
10.0	Mutual authentication shall be used to during the process to establish a connection between the email server and the wireless handheld device (certificate based authentication is desired but not currently required).	

Requirement Number	Requirement	Source of Requirement
10.1	If certificate based authentication is used between the handheld device and the email server, the handheld device certificate will not be importable to the device or subsequently exportable from the device.	
<b>Policy Management Requirements</b>		
20.0	System must centrally enforce security policies on the handheld device. The following policies shall be available:	Wireless STIG
21.0	The system administrator shall be able to select either PIN or Smart Card Login (SCL) for user authentication to unlock the device.	DoDD 8100.2, Wireless STIG
21.1	If a PIN is used to unlock the device (vice SCL), the PIN policy must meet the following requirements (all configurable by the system administrator and controlled by a centrally managed policy rule):	
21.1.1	Maximum password age (e.g. 30 days, 90 days, 180 days)	
21.1.2	Minimum password length (a range of 5 to 12 characters is the minimum requirement)	
21.1.3	Maximum Password attempts. Device will perform a Data Protection command (see Requirements 2.0 and 30.4) after a set number of incorrect passwords are entered (a range of 3-10 incorrect passwords before a Data Wipe is performed is the minimum requirement)	
21.1.4	Maximum password history (0-5 is the minimum requirement)	
21.1.5	Several different password compositions (i.e. pattern checks) should be available, to include upper and lower case letters, numbers, and special characters, to allow administrators to tailor the password policies to fit unique organizational requirements	
21.2	If SCL authentication is used for unlocking the handheld device, the SCL shall be fully interoperable with DoD PKI and CAC.	DoDI 8520.2
22.0	The handheld device has an inactivity timeout whereby the user must reenter their user PIN or Smart Card PIN to unlock the device. Shall be configurable from the range of 0 to 60 minutes, at a minimum.	Wireless STIG
23.0	The system shall control the capability of the user to install or de-install third party applications on the handheld device.	Wireless STIG
24.0	Data-at-Rest Protection	
24.1	The system shall have the capability to encrypt all user data at rest stored on the handheld device.	DoDD 8100.2
24.2	FIPS 140-2 validated encryption (AES-256 preferred; 3DES or AES required (Note, some DoD sites may require AES only)) shall be used for data-at-rest protection.	
24.3	A highly desirable feature (but not required ) is the capability to encrypt all removable storage media.	
25.0	Bluetooth requirements:  (Note, currently, Bluetooth is only authorized for handheld device connection to approved Bluetooth enabled Smart Card Readers (SCR). All other Bluetooth services are not authorized.)	DoDD 8100.2, NSA Report I332-013R-2006

Requirement Number	Requirement	Source of Requirement
25.1	Bluetooth service and profile requirements	
25.1.1	Except for the Serial Port profile, all Bluetooth services/profiles, user controls, and applications must either be removed from the host device or reliably disabled.	
25.1.2	The Bluetooth Serial Port can only be used with a Bluetooth SCR	
25.2	The system administrator shall have the capability to disable the following if not already permanently disabled:  Note: the Bluetooth features listed below will be enabled by the system/system administrator only when a Bluetooth SCR is used.	
25.2.1	-Bluetooth radio and/or Bluetooth connectable mode.	
25.2.2	-Discoverable mode	
25.2.3	-Serial Port profile	
25.3	The system shall have the following Bluetooth capabilities:	
25.3.1	Bluetooth pairing using a randomly generated passkey size of at least 8 digits	
25.3.2	Bluetooth mutual authentication immediately after the initial establishment of any Bluetooth connection between the handheld and the SCR	
25.3.3	128 bit Bluetooth encryption	
25.3.4	FIPS 140-2-certified cryptography of data-in-transit over the Bluetooth link.  Note: It expected that the data transmission between the SCR and the handheld be encrypted with FIPS 140-2 certified encryption. This encrypted data payload will then be encrypted by the 128-bit encryption provided by the Bluetooth protocol.	
25.3.5	Bluetooth devices should only use Class 2 or 3 standard radios. Class 1 radios are not permitted. Radio modifications (e.g. signal amplification, antenna modification) are not permitted.	
25.3.6	Bluetooth Device Addresses (BD_ADDRs) should not be visibly printed on the outside of the device.	
25.3.7	Random passkeys must be newly generated for each Bluetooth pairing.	
25.4	For Bluetooth SCR, the system shall have the following capabilities:  -Adjustment for the maximum Bluetooth range  Note: this a desired, but not required, feature.	
26.0	The system administrator shall have the capability to disable the following wireless services on the handheld device:	Wireless STIG
26.1	-Text Messaging (SMS)	
26.2	-MMS	

Requirement Number	Requirement	Source of Requirement
27.0	The system administrator shall have the capability to enable or disable the following PKI related configuration settings on the handheld device or alternatively, the system will provide the user the capability to accept or not accept a certificate with the following characteristics:  (Note: the desire is to have the certificate policy on the handheld device (e.g. accept/not accept certificates with specific characteristics) mirror the practice used on DoD workstations.)	Wireless STIG
27.1	-Revoked certificate use	
27.2	-Unverified certificate use	
27.3	-Untrusted certificate use	
27.4	-Non-FIPS approved algorithm used in certificate	
27.5	-Invalid certificate use	
27.6	-Unverified CRL use	
28.0	Handheld device IR port, radio (WiFi, BT, WiMax, etc.), microphone, camera, memory card port can be disabled by system central IT policy management software.  (Note: There is no requirement that the services listed above remain disabled after a hard reset (device wipe) of the PDA.)	Wireless STIG
29.0	Compliance verification. The Security system will verify that the handheld device meets compliance requirements prior to allowing a connection to the email system or network resources. Compliance requirements include the following:	
29.1	Security Policy management client installed	
29.2	Security Policy enabled	
29.3	Antivirus application installed and un-to-date (Optional)	
29.4	Operating System patches up-to-date (Optional)	
29.5	Firewall application installed and configured according to system security policy (Optional)	
<b>Handheld Device Requirements</b>		
30.0	User authentication to unlock handheld device	
30.1	The handheld device must be protected by authenticated logon using a PIN or smart card logon (SCL).	DoDD 8100.2, Wireless STIG
30.2	A user cannot bypass handheld device authentication.	
30.3	When CAC authentication is enabled, a user cannot bypass this feature and use password authentication	

Requirement Number	Requirement	Source of Requirement
30.4	When password authentication is enabled, the handheld device will automatically perform a Data Protection command ("Data Wipe" or "Data Obfuscation") after X number of unsuccessful password authentication attempts are made. The value of X is set by IT policy management control. (See requirements 2.0 and 21.0 for additional information.)	
31.0	Digital credential migration	
31.1	The handheld device shall support credential migration in a secure manner by credential owner if device is to be re-provisioned (e.g. system/application software reloaded).	
31.2	The handheld device shall support credential migration in a secure manner by credential owner when user gets a new CAC.	
32.0	Digital signing/encrypting/decrypting messages	Wireless STIG
32.1	The user shall have the capability to digitally sign and/or encrypt outgoing email messages using software or hardware based digital certificates.	
32.2	The user shall have the capability to decrypt incoming email messages using software or hardware based digital certificates	
32.3	The system shall provide a mechanism to provide certificate validation through either trusted OCSP, CRLs, or SCVP.	
32.4	The system shall support LDAP/LDAPs (as soon as practical after protocol approval). (This is the mechanism that allows the user to do ad-hoc public certificate lookups and retrievals using LDAP.)	
33.0	DoD approved antivirus software shall be operated on the handheld device (or system IT policy management software provides same function).	DoDD 8100.2
34.0	DoD approved personal firewall software shall be operated on the handheld device (or system central IT policy management software provides same function). The firewall shall be able to filter both inbound and outbound traffic based on ports, protocols, services, and IP address.	Wireless STIG
<p>Note 1: NSA/CSS Policy Manual 9-12 also does not contain sanitization guidance for Flash memory and NSA is not expected to release guidance for Flash memory for the foreseeable future. A vendor developed Flash memory sanitization maintenance utility that performs a system wipe of Flash memory, should have the following characteristics:</p> <ol style="list-style-type: none"> <li>1. Write a preset pattern</li> <li>2. Address every user addressable memory location</li> <li>3. Perform some type of verification of steps 1 &amp; 2</li> </ol> <p>There is no DoD test procedure/certification process for vendors to certify they meet these procedures.</p>		